Amendments to the Claims:

This listing of claims replaces all prior versions, and listings of claims in the instant application:

Listing of Claims:

1. (Currently amended) A method comprising:

comparing at least a portion of outbound traffic on a host computer system to at least a portion of inbound traffic on the host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system, and wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system, and further wherein the at least a portion of the outbound traffic is subsequent in time to the at least a portion of the inbound traffic;

determining if malicious code is detected on the host computer system based on the comparing; and

when malicious code is detected, providing a notification of the malicious code detection.

2. (Cancelled)

3. (Original) The method of Claim 1, wherein the comparing is performed using a similarity comparison technique.

4. (Cancelled)

5. (Original) The method of Claim 1, wherein the inbound traffic is received at the host computer system from a source port,

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

and wherein the outbound traffic is for sending to a destination port,

and further wherein the source port and the destination port are the same port.

6. (Previously presented) The method of Claim 1, wherein the inbound traffic is received on the host computer system from a source port,

and wherein the outbound traffic is for sending to a destination port,

and further wherein the source port and the destination port are different ports.

7. (Previously presented) The method of Claim 1, further comprising:

implementing protective actions.

8. (Previously presented) The method of Claim 1, further comprising:

intercepting the inbound traffic;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting the outbound traffic;

copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic; and

releasing the outbound traffic.

9. (Original) The method of Claim 8, wherein the comparing comprises:

comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic.

10. (Previously presented) The method of Claim 1, further comprising:

intercepting the inbound traffic;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting the outbound traffic;

buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic; and

if malicious code is not detected releasing the buffered outbound traffic.

11. (Original) The method of Claim 10, wherein the comparing comprises:

comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic.

12-14. (Cancelled)

15. (Previously presented) A method comprising:

intercepting inbound traffic on a host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting outbound traffic on the host computer system wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system;

copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic;

releasing the outbound traffic;

comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic;

determining if malicious code is detected on the host computer system based on the comparing; and

if malicious code is detected, providing a notification of the malicious code detection.

16. (Original) The method of Claim 15, wherein the comparing is performed using a similarity comparison technique.

17. (Original) The method of Claim 15, wherein the at least a portion of the copied outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic.

18. (Original) The method of Claim 15, further comprising:

prior to the copying the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic.

19. (Original) The method of Claim 15, wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis,

and wherein the outbound traffic is copied to the outbound traffic memory area on a per destination port basis.

20. (Previously presented) A method comprising:

intercepting inbound traffic on a host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting outbound traffic on the host computer system wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system;

buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic;

comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic;

determining if malicious code is detected on the host computer system based on the comparing;

if malicious code is detected, providing a notification of the malicious code detection; and

if malicious code is not detected, releasing the at least a portion of the buffered outbound traffic.

21. (Original) The method of Claim 20, wherein the comparing is performed using a similarity comparison technique.

22. (Original) The method of Claim 20, wherein the at least a portion of the buffered outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic.

23. (Original) The method of Claim 20, further comprising:

prior to buffering the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic.

24. (Original) The method of Claim 20, wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis,

and wherein the outbound traffic is buffered in the outbound traffic memory area on a per destination port basis.

25. (Previously added) The method of Claim 20, further comprising:

wherein if malicious code is detected, implementing protective actions.

26. (Currently amended) A computer-program product comprising a computer readable medium configured to store computer program code comprising:

a detection application for comparing at least a portion of outbound traffic on a host computer system to at least a portion of inbound traffic on the host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system, and wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system, and further wherein the at least a portion of the outbound traffic is subsequent in time to the at least a portion of the inbound traffic;

the detection application further for determining if malicious code is detected on the host computer system based on the comparing; and

when malicious code is detected, the detection application further for providing a notification of the malicious code detection.

27. (Currently amended) The computer-program product of Claim 26, the computer readable medium configured to store computer program code further comprising:

~~wherein least a portion of the outbound traffic is compared to at least a recently received portion of the inbound traffic, the at least a portion of the outbound traffic being subsequent in time to the at least a recently received portion of the inbound traffic, and~~

~~further~~ wherein the comparing is performed using a similarity comparison technique.

28. (Currently amended) The computer-program product of Claim 26, the computer readable medium configured to store computer program code further comprising:

wherein if malicious code is detected, the detection application further for implementing protective actions.